UDC: 004.8:336.71
005.334:004.8
DOI: 10.69899/limes-plus-en-24212-3025s
Original scientific work

AI IN THE FINANCIAL INDUSTRY: HOW TO PREVENT DATA BREACHES

***Aleksandar Šević*[1]**
TCD, Trinity Business School, Dublin, Ireland
Information Technology School – ITS, Belgrade, Serbia
***Željko Šević*[2]**
International University of Applied Sciences, Erfurt, Thuringia, FR of Germany

Abstract: *The EU lags behind major US and Asian competitors in information security expenses per IT spending or employee. Compared to other areas of economic activities, financial institutions seem to be more complacent regarding potential system breaches. However, they are also better equipped to quickly identify inconsistencies because their infrastructure seems comparatively less complex. With the prospective application of NIS 2 Directives, it is imperative to examine the challenges financial institutions face with the current increase in AI capabilities that hackers and other malevolent actors could use without impunity if proper countermeasures and systems are not deployed. In this study, we provide an overview of challenges that financial institutions could face, but we also discuss solutions, such as advancements in generative AI products or the widespread application of behavioral biometrics, which should increase the reliability of online activities and prevent the abuse of personal data on a*

1 a.sevic@tcd.ie; aleksandar.sevic@its.edu.rs
2 Zeljko.Sevic@IU.org

broader scale. Apart from specific company solutions, we provide a discussion platform for government decision-makers.

Keywords: *artificial intelligence, banking, financial institutions, cybersecurity, behavioral biometrics.*

1. INTRODUCTION

By 17 October 2024, the EU member states are required to adopt measures necessary for the implementation of the NIS 2 Directive (EU 2022/2555). It replaces the NIS Directive from 2016 to ameliorate cybersecurity and establish reporting requirements across various sectors. In addition, the Digital Operation Resilience Act (DORA), adopted in September 2023, is sector-specific and takes precedence in some areas over the NIS Directive for financial entities (NIS 2, 2023).

Following these legal requirements, EU banks and other financial institutions should implement technical, operational and organizational measures to secure the network and information systems. While there may be occasional incursions by hackers, not only via bank servers but also via ATMs, it is also essential to underscore that the increase in online banking activities, which allowed for the closure of offices, decline in the workforce, and the reduction of the ATM network, also contributed to an increase in identity thefts and inappropriate money transfers.

While comprehensive antivirus protection is essential for financial institutions, it is also evident that the negligent approach to security by banking clients represents one of the stumbling blocks preventing the creation of a robust system. While the use of PINs, passwords and cards is still prevalent, there is an apparent shift among cybersecurity experts to the implementation of biometrics that are supposed to be resilient to purchase, robbery, duplication or counterfeiting (Marani et al., 2023). If there is malevolent access to passwords

or cards, the same could be replaced as many times as necessary, but the low entropy of fingerprints that are compromised by criminals, and more prone to be repeated in the general population, would force banks to scan other biometrics, such as face or irises, which are more person-specific.

With the advancement of AI, especially in natural language processing (NLP) or drawing, the proliferation of fake news or videos has become available to amateurs without any specialized knowledge in coding or design. This would imply that criminal or state-sponsored actors are trained and equipped to create impeccable announcements, web designs, photos or videos. If this is the case, banks and other financial institutions must move to the next step of behavioural biometrics that would recognize patterns using deep machine learning. However, since humans change behavioural patterns with age, the AI must be able to identify these shifts, as well.

In the continuation of the paper, we discuss the growing relevance of artificial intelligence, and then in Section 3, we discuss various types of AI-driven frauds. In Section 4, we shall discuss the improvements in the financial services in the near future and then finalize the study with concluding remarks.

2. AI MATTERS

Artificial intelligence can carry out human tasks, and it is achieved by collecting, interpreting and learning from externally provided data (Craft, 2011; Haenleing and Kaplan, 2019). Apart from the popular images and movies that captivate public imagination, be it positive or negative, regarding AI, we face a gradualist view that machines will help humankind replace rather dull and repetitive jobs with a shift towards group work with machines leading to the ultimate augmented intelligence (De Cremer and Kasparov, 2021). This postulate is based on the fact that machines are fast but lack emotional intelligence, intuition and cultural sensitivity. If AI could mimic these features, then human labor would be in peril of being completely replaced by machines. Should these concerns be voiced by leading physicists, such as Stephen Hawking or

businesspersons, such as Bill Gates, the threat is incomparably more resonating among the audience (Kumar and Choudhury, 2022; Rawlinson, 2015). The speed of AI development and adoption will determine the rate of human obsolescence and its replacement.

Even at the current level of AI development, where almost none of the more profound human-like features can be teased out of the machines, the advancements in language processing, image enhancement and voice recognition create opportunities and challenges for businesses and regulators. Financial institutions have already dabbled in using robo-advisors, but with the advancement in NLP, the ability to provide quality customer services has tremendously improved. Law departments would deploy self-learning neural networks to scan regulations not only in the host country but globally and secure manageable answers at a fraction of an earlier timeframe. Banks already evaluate customers more comprehensively with a vast speed improvement, while the search for AI-enabled company headquarters or other facilities would reduce insider frauds, but also, in exchange for some additional loss in privacy, employees should be able to enter the building, enjoy the working environment and leave the premises under constant surveillance, which, in turn, would reduce other, more visible, control points (Noonan, 2023). Finally, we may witness a decline in the hiring rates as human labor becomes less useful for employers.

Where did this drive to boost productivity originate? Firstly, the goal of reaping the benefits of newcomers into the market is enticing enough for banks to implement AI-driven changes. Secondly, the threat by FinTech companies has become a reality, and if conservative policies are implemented, banks will run the risk of becoming moribund giants of inefficiencies. Thirdly, the business world yearns to face years of significant productivity increases. Except for 1997–2004, the IT-driven growth has failed to re-appear. The advancement might have been limited to specific areas of human activity that did not convert into growth, or the measuring was incorrect (Brynjolfsson et al., 2019). The additional claim

by these authors that some technological advancements such as nuclear power or flying cars failed to become as omnipresent is a moot point because AI is a game changer, perhaps even the ultimate chapter of human development, because it complements, improves on and then it is forecasted to outshine humans in almost every aspect imaginable.

It is doubtful whether similar claims would have been made should ChatGPT in 2019 instead of 1.5 billion parameters have as much as 175 billion, the same as ChatGPT-3 only four years later. This improvement did not materialize without costs. The ChatGPT training had a strong impact on the environment, with 502 metric tons of carbon emitted. Adding ChatGPT to the Bing search engine increased the consumption per search by five times. So far, global data centers have used approximately one percent of global electricity annually, and with the recent breakthrough, the relative electricity consumption rate will have doubled by 2030 (Cho, 2023). An increase in parameters allows artificial neural networks to perform tasks more accurately and rapidly, but it also increases energy consumption. The reduction of this negative trend could be achieved by exacting less accuracy for tasks where high precision is not relevant or by making further inroads in the spiking neural network research where calculations could be up to 280 times less energy intensive since neurons are either active, when necessary, or remain inactive without energy consumption (Dora, 2024).

While the underlying processes of AI neural networks are known and heavily researched, the ramifications of AI on humanity are still unknown, implying that the regulatory framework is still to be implemented. The hype has not subsided; leading, mainly US, companies are jockeying for the top position in this realm, but it does not mean that many other OECD countries have not already outlined some general strategies for AI advancements. In 2017, China adopted "The Next AI Development Plan", aiming to become the global innovation center by 2030. Soon after that, the EU in 2018 and the US in 2019 promoted the development or leadership in AI. The amount of committed investments in China is matched

by the ability of US companies to raise capital in highly liquid domestic markets, but the ringfenced outlays for AI in France, Germany or the UK, as one of the leading European countries, are comparatively smaller (Figure 1) (Sheppard et al., 2018). The strength of Europe originates in its talent (Figure 2). Suppose Sam Altman, the controversial CEO of OpenAI, is correct in estimating that investments in AI will range between several hundred billion US$ and US$ 7 trillion. In that case, the dominating players will be in the US and China, not in Europe (Cornish, 2024).

Figure 1. Investment in AI companies

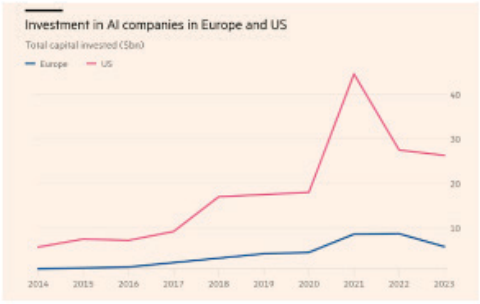
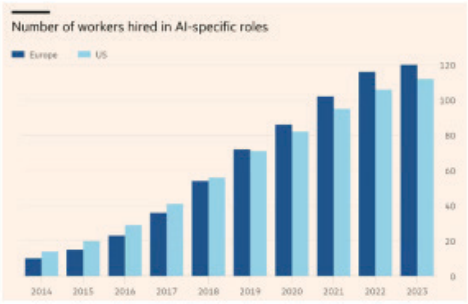


Figure 2. Number of workers hired



Source: Financial Times

On 13 March 2024, the European Parliament passed the first Artificial Intelligence Act in the world, aiming to protect safety, health and individual rights, but not to stem the growth in AI use in the EU. The Act prohibits using biometric categorization systems at work or in education to recognize emotional states or other vulnerabilities of subjects of interest. Social scoring or predictive policing is not allowed, as well. The areas to be explored in our paper will be placed under the aegis of high-risk AI systems that could be deployed in training, employment, private or public services. Under the new legislation, deploying detailed risk management, keeping logs, ensuring transparency and accuracy, and involving human oversight without exceptions are necessary.

Manipulating video, images or voice content must be clearly marked, and the more powerful general-purpose AI system will require more frequent and comprehensive reviews, coinciding with the level of damage it could inflict. The legislative act pays special attention to the certification process, taking into account technological progress, which means that at some point, high-risk AI systems may be evaluated as such (Artificial Intelligence Act, 2024). As a supranational organization, the EU legislation has to consider all member countries' interests, with specific exceptions, for instance, in Ireland, due to its relationship with the UK (Shmuha, 2021). It is a big step forward and should contribute to the preservation of fundamental rights that are enshrined in the previous EU legislation, but shortly after the adoption, Canada, Singapore and UAE are reported to have been approaching European AI start-ups and showering them with tax breaks, golden visas and other benefits (Criddle and Cornish, 2024). The UK has also joined the queue of bidders, but the closer the company is to the EU market, the less chance it has of being excluded from the EU Act if operations are conducted on the continent. In October 2023, the US President signed the Executive Order on "Safe, Secure, and Trustworthy" Artificial Intelligence, aiming to require various government agencies to prepare task lists ranging from 90 days to a year in the areas of safety and security, the use of AI by the US government, privacy protection, consumer protection and civil rights and equality (Rubin and Manes, 2024).

3. AI-DRIVEN FRAUDS

ChatGPT 3 from OpenAI, as the most conspicuous representative of a league of natural language processing products emanating from other competitors such as Microsoft Azure, Stanford CoreNLP, Google Cloud or IBM Watson, allowed many actors across the globe to maintain almost simultaneous "communication" with a machine. The 175 billion parameters allowed it to predict words at a speed rate and the context in which humans could assume that there is an intelligent counterpart, although somewhat constrained by engineers

and puzzling perceptions of ethics, on the other side. However, it was discovered very quickly that homework, essays and reports could be created within a very short period, thereby cutting the time necessary to complete the task. Then, the Dall-e 2, another product by OpenAI, offered enviable image generation. If, in such an abundance of neural network solutions, even amateurs at a fraction of the cost could manipulate photos, voices, videos and allegedly original documents, then the stage for the next-generation AI-driven fraud is unambiguously set.

The financial institutions and their customers will increasingly face threats such as:

a) The proliferation of fabricated documents used in the process of identification or application submissions. The challenge is that these copies are so well made that internal checks and balances are insufficient to spot them.
b) Fake voices over the phone or chat platforms could be used to impersonate close relatives, trick the person into providing payments, or mimic the voice of an abducted person in search of a ransom payment. If these are used to represent financial experts or managers involved in passing relevant decisions, a lack of trust, insecurity, or fraud could be perpetrated.
c) Fake videos could be obtained from the dark web for US$150 via WormGPT, FraudGPT, DarkBART or similar platforms. The deployment for phishing or ransomware is then further facilitated thanks to a multitude of products tailored for criminals. If videos impersonate celebrities, the scam becomes more convincing, and criminals can achieve targeted financial results with a relatively small sample of randomized victims. It may not be necessary to apply strategies to a broader audience, which may keep it outside the public's eye for longer.
d) The easiest access to sensitive datasets is for company insiders. If artificial intelligence allows them to misuse company or client accounts with impunity, the incidence of breaches will increase.

e) AI-powered algorithms in capital markets should be able to collude without the explicit violation of market watchdogs' rules. If price-trigger strategies are followed, algorithms switch from exploration to collusion with similar products, and at some point, significant profits will be recorded. Even in a high-noise environment where innovative trading strategies are difficult to follow, AI-supported algorithms demonstrate similar biases and again reap substantial profits. These processes may be already under way in capital markets and their final impact on markets and society is yet to be analyzed.

f) Social engineering attacks account for four-fifths of all IT breaches and exploit human weaknesses by abusing psychological techniques. The AI-enhanced content via chatbots, voice generation, and fakes could make these attacks highly convincing and sophisticated, boosting the success rate.

g) High-risk AI systems will become increasingly complex and brandish capabilities to access and manipulate personal data on a large scale. If these data uses cannot be ringfenced, there is a significant likelihood of leaking information to actors who should never be designated to have access (Venkataramakrishnan, 2024; Jaskiewicz, 2023; Dou et al., 2023; Zvelo, 2023; Shen, 2023).

4. FINANCIAL SERVICES OF THE NEAR FUTURE

Compared to transportation and aviation, communications, utilities and government, financial services have expressed the smallest increase in successful cyber attacks but also the second least concern about cyber warfare, trailing only behind communications. Despite this striking confidence, financial actors are confident that the majority of future attacks will originate in cloud services (identified by 46% of respondents), remote employees (39%) and insecure virtual private networks (VPN) (37%) (Bridewell, 2023). Since 2018, the cybersecurity risk, closely followed by the geopolitical risk, has become a major concern for

UK banks (Bank of England, 2023). These attitudes reflect the challenges that data-driven companies are about to face.

McKinsey outlines multiple steps that should be implemented by the data-driven company by 2025. The timeframe looks pretty ambitious, but the goal is not unfeasible given the recent drive to include artificial intelligence in as many company activities as possible. Data is expected to be omnipresent and effectively used in the decision-making process. In the analysis process, thanks to cloud services and real-time access, financial experts will use virtual and augmented reality to make more comprehensive decisions in a multidimensional space. Thereafter, it is necessary to integrate various databases into a single "360-degree view" to properly understand the needs of banking customers and support them by offering rankings to companies they invest in. The provision of and access to securely kept data should be rapid, and all relevant applications submitted by customers must be quickly processed. Finally, the chief data officers will be able to monetize services related to data manipulation (McKinsey Digital, 2022).

The generative AI will improve automation, especially in tedious processes in banks, and it will also augment productivity and accelerate innovative drives. However, with the broader use of generative AI, humans are still a valuable control factor, because these systems are capable of producing impeccable reports with erroneous or non-extant sources. The hallucinations based on model predictions rather than reality could be devastating if distributed inadvertently (Agrawal et al., 2022). Then, the outcomes of genuine and nefarious actors' actions could be indistinguishable.

Banks were the early adopters of robo-advisors, and it is to be expected that natural language processing will allow for more human-like interaction with customers, not only via online chats but also via the phone. AI-assisted robo-advisors reduce confirmation and hindsight biases routinely demonstrated by human financial advisers (Hasan et al., 2024). For the latter option, i.e.

phone conversation, further improvements are still expected, because the latency in responding and the comprehensiveness of provided answers may not be satisfactory. Moreover, if the system were prone to hallucination, then the customer's trust could be destroyed. The use of Robotics Process Automation will reduce the time necessary for completing repetitive and relatively simple tasks in the back office, which will either reduce the workforce or free up employees' time for more complex tasks (Sushant Das et al., 2024).

Banks pay special attention to streamlining credit approvals. At the same time, it is one of the high-risk AI areas to which the EU Act on Artificial Intelligence would pay special attention. The data collection and analytics, as the cornerstone of the AI breakthrough in this domain, or behavioural biometrics cannot be used to exploit the weaknesses or violate the fundamental rights of the applicant, despite the necessity to examine a multitude of applicants' features to secure the repayment of the loan. Another problem is the accuracy of machine learning, which is a significant concern for banking regulators. One of the solutions could be to refocus from accuracy to optimizing some other specific functions that will boost bank profits (Gramespacher and Posth, 2021).

Ultimately, the banks have to increase investments in preventing fraud and improving the security of collected datasets. The use of AI in data-driven banks will tremendously increase the necessity of evaluating, sharing, and storing datasets, thereby creating many points where potential vulnerabilities may be exploited.

The first step is to allow future customers to verify who they are. In bank branches, the photo from the document would be compared with a person standing in front of the clerk, but it has been shown that humans are not good at matching old photos with 3D appearances. Fintech companies, such as Wise or Revolut, request the submission of real-time photos, passports or other documents via the app during online registration, which is a rich source of information for providers. Phone numbers, email accounts, phone switching or

spending patterns are all useful indicators for evaluating clients (Noonan, 2023). Nevertheless, financial institutions have to move a step further and explore the use of behavioral biometrics. In the first half of 2023, frauds committed by CEOs, banks or law enforcement officials in the UK, thanks to voice generation or video deepfakes, amounted to almost 9 per cent out of £580 million (Quinio, 2024). Payment service providers in the UK have a vested interest in improving the safety of apps, because starting from October 2024, the cost of a single app fraud must be equally shared by sending and receiving payment service providers up to the maximum amount of £415 (PSR, 2023). Faked videos can be used for identification purposes via apps, and if these are difficult to recognize by bank verifiers, one has to explore the advancements in technologies that will recognize single persons among many more accurately.

The system may assume the account has been hacked if users demonstrate unusual browsing patterns. It is also possible to embed watermarks in faked videos for verifiers to recognize them, but the problem is that these watermarks could be hacked, and if it is attached to an original video, the entire process is compromised (Quinio, 2024).

So far, banks have been constrained to use physiological biometrics such as fingerprint or face recognition. Still, the next step involves using behavioral biometrics, such as swiping, keystroke dynamics, gait activities, browsing or touching (Kokal et al., 2024). The modalities of the client's behavior represent a rich source, but it also puts this mode of authentication on a collision course with current and future legal acts. If it becomes quite easy for hackers to compromise accounts, financial services must introduce a so-called continuous authentication to prevent interruptions in service provision and reduce harm. The more modalities the authentication process examines, the more effective it is. However, the moment the data are stored in the server, there is a high likelihood for someone to access the private data unlawfully. One of the solutions could be hashing or returning the authentication data to the client without even letting the server know what indices are used during the authentication (Baig et al.,

2023). Personal data can also be protected by de-identification that modifies and obscures information from the public prying eye (Shopon et al., 2021).

5. CONCLUDING REMARKS

Financial institutions demonstrate a comparatively higher level of confidence vis-à-vis other industries in brandishing their ability to deal with cybersecurity threats. The lack of a complex structure allows their IT experts to pinpoint inconsistencies earlier. The move to the data-driven business environment, strongly dominated by AI-assisted platforms, will further reduce this timeframe, optimize timeframes and allow employees to focus on more complex assignments.

Europeans have made a quantum leap by adopting a standalone Artificial Intelligence Act in March 2024, when major economies struggle to attract the best global talent and reinvent themselves as AI innovation hubs. This may be a risky strategy if the industry, entirely in its early stages, perceives the scope of regulation as onerous. As claimed in this paper, non-EU countries have already attempted to poach EU start-up companies, offering them an unbridled research environment and a range of incentives. So far, other countries have decided to expand the discussion or try to regulate the area by amending existing legal acts. Ultimately, supranational standards will be agreed upon, but no one can accurately predict what the AI success story by countries and regions will look like by then. Europe may have an educated talent pool, but China and the US offer better financial support. Finally, many contenders for the third and other positions are on the leaderboard.

The advancement of AI-modified voices, photos and videos allowed malicious actors, even those with minimal technical skills, to launch highly sophisticated attacks on individuals and institutions. Fake personalities or relatives could illicitly access accounts or persuade people to transfer money to them. Wary of these challenges, the UK regulators have already accepted the

legislation that forces sending and receiving payment service providers to cover damages incurred via the application equally.

AI-generated threats are multifaceted, but banks and other financial institutions are urged to take advantage of the latest artificial intelligence advancements. AI will be omnipresent, tasks will be quickly resolved, data will be available for all relevant parties in a quick manner, and productivity will finally increase considerably. However, with the usage of cloud computing and a flexible work environment, financial actors predict that the primary venues for hackers' attacks will come via these two entry points. If authentication is compromised frequently, it is necessary to advance the use of behavioral biometrics while also paying attention to preserving each client's privacy.

REFERENCES

1. Agrawal, A., Ellencweig, B., Sood, R., Tam, M. (2022). Gen AI: A guide for CFOs. McKinsey and Co.
2. Artificial Intelligence Act 2024. P9_TA(2024)0138, European Parliament 2019–2024.
3. Baig, A.F., Eskeland, S., Yang, B. (2023). "Privacy-preserving continuous authentication using behavioral biometrics." International Journal of Information Security 22: 1833-1847. https://doi.org/10.1007/s10207-023-00721-y
4. Bank of England (2023). Systemic Risk Survey Results- 2023 H2.
5. Brynjolfsson, E, Rock, D., Syverson, C. (2019). "Artificial intelligence and the modern productivity paradox: A clash of expectations and statistics." In Agrawal, A., Gans, J., Goldfarm A. (Eds.), The economics of artificial intelligence: An agenda. National Bureau of Economic Research, The University of Chicago Press: Chicago and London.
6. Bridewell (2023). Cyber security in critical national infrastructure organizations: Financial Services, Research Report.

7. Cho, R. (2023). "AI's growing carbon footprint." State of the Planet, Columbia Climate School, Climate, Earth and Society.
8. Cornish, C. (2024). "Abu Dhabi in talks to invest in OpenAI chip venture." Financial Times, 15 March, 2024.
9. Crafts, N. (2021). "Artificial intelligence as a general-purpose technology: A historical perspective." Oxford Review of Economic Policy 37 (3): 521–536. https://doi.org/10.1093/oxrep/grab012
10. Criddle, C., Cornish, C. (2024). "Rival nations seek to poach top UK and European AI start-ups." Financial Times, 20 March, 2024.
11. De Cremer, D., Garry K. (2021). "AI should augment human intelligence, not replace it." Harvard Business Review, Winter Special Issue: 97–100.
12. Dora, S. (2024). "AI has a large and growing carbon footprint, but there are potential solutions on the horizon." The Conversation.
13. Dou, W.W., Goldstein, I., Ji, Y. (2023). "AI-powered trading, algorithmic collusion, and price efficiency." Jacobs Levy Equity Management Center for Quantitative Financial Research paper. http://dx.doi.org/10.2139/ssrn.4452704
14. Gramespacher, T., Posth, J. A. (2021). "Employing Explainable AI to Optimize the Return Target Function of a Loan Portfolio." Frontiers in Artificial Intelligence, 4(June): 1–13. https://doi.org/10.3389/frai.2021.693022
15. Haenlein, M., Kaplan, A. (2019). "A brief history of artificial intelligence: On the past, present, and future of artificial intelligence." California Management Review 61 (4): 5–14. https://doi.org/10.1177/000812561986492
16. Hasan, Z., Vaz, D., Athota, V.S., Maturin Desire, SS, Pereira, V. (2024). "Can artificial intelligence (AI) manage behavioral biases." Journal of Global Information Management 31 (2): 1–18. doi: 10.4018/JGIM.321728
17. Jaskiewicz, R. (2023). "Unleashing the power of AI in secured finance industry: A journey into change and evolution." The Secured Lender (July-August): 64-65.

18. Kokal, S., Vanamala, M., Dave, R. (2023). "Deep learning and machine learning, better together than apart: A review on biometrics mobile authentication." Journal of Cybersecurity and Privacy 3: 227–258. https://doi.org/10.3390/jcp30200134
19. Kumar, S., Choudhury, S. (2022). "Humans, superhumans, and superhumanoids: Debating Stephen Hawking's doomsday AI forecast." AI and Ethics 3: 975–984. https://doi.org/10.1007/s43681-022-00213-0
20. Marani, M., Soltani, M., Bahadori, M., Soleimani, M., Moshayedi, A. (2023). "The role of biometrics in banking: A review." AIRO, EAI. DOI: 10.4108/airo.3676
21. McKinsey Digital (2022). The data-driven enterprise of 2025. McKinsey and Company.
22. NIS 2 (2023). Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive).
23. Noonan, L. (2023). "CEOs relish prospect of AI boost to productivity: Artificial intelligence banks expect the technology to increase efficiency." Financial Times, 18 September 2023.
24. PSR (Payment System Regulator) (2023). Policy statement: Fighting authorized push-payment scams: Final decision, PS 23/4, December.
25. Quinio, A. (2024). "UK banks prepare for deepfake fraud wave." Financial Times, 19 January, 2024.
26. Rabesandratana, T. (2018). "Europe moves to compete in global AI arms race." Science 360 (6388). doi: 10.1126/science.360.6388.474-a.
27. Rawlinson, K. (2015). Microsoft's Bill Gates insists AI Is a Threat. BBC News. Available online: https://www.bbc.co.uk/news/31047780 (accessed on 15 March 2024).
28. Rubin, H., Manes, A. (2024). "President Biden Signs Executive Order on 'Safe, Secure and Trustworthy' Artificial Intelligence." The Computer and Internet Lawyer 41 (2): 13–14. ISSN: 1531–4944

29. Shen, L. (2023). "World news: AI-driven fraud makes news in China." Wall Street Journal, Eastern ed., NY 5 June, 2023.
30. Sheppard, L.R., Karlen, R., Hunter, A.P., Baliero, L. (2018). "Artificial intelligence and national security: The importance of the AI system." A Report on the CSIS Defense-Industrial Initiatives Group, Center for Strategic & International Studies.
31. Shmuha, N. A. (2021). "From a 'race to AI' to a 'race to AI regulation': Regulatory competition for artificial intelligence." Law, Innovation and Technology 13 (1): 57–84. https://doi.org/10.1080/17579961.2021.1898300
32. Shopon, M., Tumpa, S.N., Bhatia, Y., Pavan Kumar, K.N., Gavrilova, M.L. (2021). "Biometric systems de-identification: Current advancement and future directions." Journal of Cybersecurity and Privacy 1: 470–495. https://doi.org/10.3390/jcp1030024
33. Sushant Das, S., Manohar, A., Jawajala, R.P., Dhanalakshmi, K., Jadhav, M., Raje Sisodia, D. (2024). "AI application in personalized marketing and customer engagement in the retail banking industry." Academy of Marketing Studies Journal 28 (2): 1–10.
34. Venkataramakrishnan, S. (2024). "AI heralds the next generation of financial scams." The Financial Times, 19 January, 2024.
35. Zvelo (2023). The role of AI in social engineering. Available at: https://zvelo.com/the-role-of-ai-in-social-engineering (Accessed on 18 March 2023).